2

ESC-TR-93-309

MTR 93B0000095

Proposed Network Security Policy for Integrated Tactical Warning and Attack Assessment System

By

L. J. LaPadula

September 1993

Prepared for
System Program Director
Cheyenne Mountain Complex SPO
Electronic Systems Center
Air Force Materiel Command
United States Air Force
Hanscom Air Force Base, Massachusetts

Project No. 4370
Prepared by
The MITRE Corporation
Bedford, Massachusetts
Contract No. F19628-89-C-0001

Approved for public release;
distribution unlimited.

When U.S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Do not return this copy. Retain or destroy.

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.

Gerard R Cavallo

GERARD R. CAVALLO, CAPT, USAF
Chief, Systems Performance
Cheyenne Mountain Complex SPO

FOR THE COMMANDER

Michael C Mushala

MICHAEL C. MUSHALA, COL, USAF
System Program Director
Cheyenne Mountain Complex SPO

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1993	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE

Proposed Network Security Policy for Integrated Tactical Warning and Attack Assessment System

5. FUNDING NUMBERS

F19628-89-C-0001
4370

6. AUTHOR(S)

LaPadula, Leonard J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

8. PERFORMING ORGANIZATION REPORT NUMBER

MTR 93B0000095

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

System Program Director, Cheyenne Mountain Complex SPO
Electronic Systems Center (ESC/SRE)
Hanscom AFB, MA 01731-3010

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

ESC-TR-93-309

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Integrated Tactical Warning and Attack assessment (ITW/AA) system is a networked system of systems that collects, processes, and produces information, including classified.data, in.support of missile, air, and space attack warning missions. As with any mission-critical network, ensuring confidentiality and integrity of its information is necessary to support the mission and requires a network information handling policy. This document gives such a policy for the networked automated information systems of the ITW/AA system. Since the successful application of an information handling policy to a system depends on its suitability for the target system, this proposed ITW/AA network security policy takes into explicit account the intercomputer networking topology of the current ITW/AA network. At the same time, appropriate generalizations and abstractions make the policy suitable for future stages of the network. At present, the policy can serve as the baseline for assessing security risk associated with operating the current network.

14. SUBJECT TERMS

Information Systems Security
Network Security Policy
ITW/AA
Risk Reduction
Network Security Management and Auditing

15. NUMBER OF PAGES

72

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT SAR

ACKNOWLEDGMENTS

This document has been prepared by The MITRE Corporation under Project No. 4370, Contract No. F19628-89-C-001. The contract is sponsored by the Electronic Systems Center, Air Force Materiel Command, United States Air Force, Hanscom Air Force Base, Massachusetts 01731-3010.

Captain Robert Pierce of AFSPACECOM/SCXS, Captain James Hiller of AFCSC/SRMC, and Ms. Jane Cappe of AFCSC/SRMC provided extensive comments, discussion of issues, and helpful suggestions during the development of this report.

Ms. Deborah Bodeau, Mr. Fred Chase, and Mr. Robert Goldsmith of the MITRE Corporation established the technical basis for this report in an earlier work and worked with the author over many months in resolving issues addressed in this document.

For their reviews that they provided from time to time I am grateful to the following MITRE employees: Ms. Harriet Goldman, Mr. Ronald Bass, Mr. Donald Clark, Ms. Deborah Gray, and Mr. Michael Michnikov.

Finally, my special thanks to Mr. Ernest Perelmuter of the MITRE Corporation, who provided consistent, clear project guidance on this effort and carefully reviewed the report, more than once, to assure its consistency with project objectives and quality standards.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1

INTRODUCTION

The Integrated Tactical Warning and Attack Assessment (ITW/AA) system, a major defensive system performing attack warning missions, is a networked system of systems that collects, processes, and produces mission-relevant information. Because of the nature of the mission, much of the ITW/AA mission information is classified, generally at the SECRET level. National security policy requires tha: the confidentiality and integrity of this information be ensured to support the mission fully. There are many aspects to this, including physical security of facilities, personnel security, administrative support measures, and computer security measures, to mention just a few. One major aspect that we single out for consideration is the network security needed to support the mission. Although the various components of the network are covered by their individual security policies, a policy covering the interactions of the multitude of components is needed to ensure that security is comprehensive and consistent. Thus, the ITW/AA network needs a network information handling policy.

This document proposes such a policy for the networked automated information systems of ITW/AA and the communications systems they employ. Since the successful application of an information handling policy to a system depends on its suitability for the target system, the policy takes into explicit account the intercomputer networking topology of the current ITW/AA network while appropriate generalizations and abstractions make the policy suitable for future stages of the network.

1.1 BACKGROUND

The ITW/AA missions are warning and assessment of missile, air, and space attacks. This "system-of-systems" network has many mission systems, separately accredited, cooperatively carrying out tactical warning and attack assessment missions. Mission systems are either core systems or affiliated systems.

- Core system: an automated information system (AIS) having a primary function to do one or more of the ITW/AA missions.

- Affiliated system: an AIS that does an ITW/AA mission as a secondary mission. The Air Force Global Weather Central (AFGWC) system, which provides aerospace environmental data for ITW/AA missions, is an affiliated system.

In addition, nonmission systems participate in the ITW/AA intercomputer networking for certain classes of information, such as the Smithsonian Astrophysical Observatory and the STRATCOM-unique CCPDS-R. Any system that participates in the ITW/AA intercomputer networking for information exchange is called a participating system, whether a mission or a nonmission system.

Air Force Space Command (AFSPACECOM) is the designated approving authority (DAA) for most of the mission systems. Strategic and Tactical Command and several other DOD components have approval authority for some systems. Canada and the United Kingdom will own and operate several mission systems.

1.2 RATIONALE FOR SECURITY POLICY

Integrated Tactical Warning and Attack Assessment (ITW/AA) constitutes a major defensive system performing attack warning missions. It collects and processes several sources of information and produces various summaries, reports, and messages, many of them classified. As with any information processing enterprise, ensuring confidentiality and integrity of its information is of great importance to carrying out its mission effectively. Since the ITW/AA system spans several authority domains and encompasses widely disparate computer systems, effective implementation of measures for information protection requires a network information handling policy. We refer to this policy as the ITW/AA network security policy.

Security engineering for the ITW/AA network comprises several related topics.

- Network Security Policy
- Risks and Recommendations
- Network Accreditation Management Plan
- Network Security Architecture
- Security Label Standards

These topics together give a comprehensive treatment of network security functions and requirements. Each focuses on a specific aspect of operation and management of the ITW/AA network.

- Network Security Policy — This theme deals with the ITW/AA network security policy—an information handling policy that gives a basis for risk assessment and guides development of new capabilities.

- Risks and Recommendations — This theme involves the results of risk assessment, providing guidance for incremental improvements and programmatic developments.

- Network Accreditation Management Plan — This theme comprises a plan for accrediting the ITW/AA network in light of known risks and desired security architectural improvements.

- Security Architecture — This theme embodies plans for evolving the ITW/AA network from its current security posture to improved positions.

- Security Label Standards — This theme deals with standards for security labels on information that is transported on the ITW/AA network.

1.3 TERMINOLOGY

The proposed network security policy in the appendix and the discussion about that policy in the body of this document rely heavily on technical words and phrases. We have used well-known technical terms with their usual meanings and have added a number of additional terms to our terminology specifically for this ITW/AA network security policy. These additional terms are based on common words and phrases with their specialized meanings given in the glossary of this document. Thus, we urge the reader to become familiar with the glossary, which defines all technical terms, to ensure understanding of the policy requirements.

1.4 ORGANIZATION OF THIS DOCUMENT

The rest of this document has two sections, followed by an appendix, a glossary, and an index.

- Section 2 gives a preamble for the network security policy, covering background and rationale for policy requirements and the technical approach.

- Section 3 discusses the technical approach used in defining the network security policy given in the appendix. The discussion describes the view of the ITW/AA network that is used and summarizes the major characteristics and key features of the network security policy.

- The appendix contains the formal specification of the network security policy, giving policy requirements in three categories.

  - Network security management requirements — these cover roles and responsibilities, system accreditation, attaching to the network, audit, and contingency operation.
  - Technical requirements for prevention of unauthorized disclosure — these are labeling, network interface, input channel, and output channel requirements.
  - Technical requirements for maintaining integrity — these are data integrity, protocol integrity, and authentication requirements.

- The glossary defines acronyms used and gives an extensive set of definitions for reserved and technical terms.

- The index gives page references to material by subject, alphabetically organized.

SECTION 2

PROLOGUE FOR THE NETWORK SECURITY POLICY

2.1 APPLICABILITY AND SCOPE

The term "automated information system (AIS)" means, as is usual, a collection of hardware, software, and firmware configured to process data electronically. This term should be understood to be quite general in this document. In the proposed network security policy of appendix A, an AIS may be a single computer or workstation or an aggregate of computers, workstations, servers, and communications equipment identifiable as a single system, such as a local area or wide area network.

The policy for network security applies to all ITW/AA-related information exchange. The network security management portion of the policy generally applies only to the mission AISs of the ITW/AA network, while the technical nondisclosure and integrity requirements apply to all mission systems and extend out to the network interfaces of nonmission systems. Generally, the scope of the network security policy extends to all instances of networking capabilities and systems whose compliance with the policy the ITW/AA Network DAA will consider. The policy's scope is explained in detail later in section 3.

The network security policy includes

- General network management requirements to facilitate correct and reliable nondisclosure and integrity protection — these requirements cover
  - roles and responsibilities
  - individual system accreditation
  - conditions for an AIS's participation in the network
  - network audit and
  - contingency operation
- Requirements for protection of information from unauthorized or accidental disclosure during intercomputer information exchange — these nondisclosure or secrecy requirements reduce the risk of unauthorized disclosure of ITW/AA information.
- Requirements for protection of information from unauthorized or accidental modification, insertion, or deletion during intercomputer information exchange — these integrity requirements ensure that secrecy mechanisms function properly and that mission information is not altered in transiting from one ITW/AA system to another.

The network security policy gives guidance for designing and operating the network securel:. Other security policies and standards, which are outside the scope of this document, must also be applied to minimize network risk. For example, if physical cabling between nearby AISs assumes physical protection, then relevant policy for physical security of cabling must be applied.

Security requirements for individual AISs are specified by regulation. The bibliography of this document has a list of relevant ones. The policy specified in the appendix of this document complements the regulations for individual AISs because it states the requirements for information exchange among the various mission systems of the ITW/AA network and between a mission system and other, nonmission systems. It imposes additional controls on the individual mission AISs and requires the ITW/AA Network DAA or designees to enforce administrative controls.

2.2 POLICY OBJECTIVES

The office of AFSPACECOM/SC has identified the following policy objectives.

Policy Objective 1. The ITW/AA Network DAA will accredit the ITW/AA network to operate at an acceptable level of risk in accordance with DODD 5200.28 [1], Air Force Regulation (AFR) 205-16 [2], and the Space Command Supplement to AFR 205-16 [3].

Assessment of risk involves three factors.

- The likelihood that someone will try to exploit a vulnerability in the ITW/AA network
- The likelihood that such an attempt will have an impact
- The severity of that impact. There are three types of impact:
    - disclosure of classified or sensitive-but-unclassified data to an unauthorized individual
    - denial-of-service—inability of the ITW/AA network to support one or more of its missions in a timely manner
    - resource corruption—loss of correctness of the data and/or algorithms needed by one or more mission systems to support one or more of the ITW/AA missions correctly. Ambiguity in distinguishing among real, test, and exercise data would be a special case of resource corruption.

The ITW/AA Network DAA will assess the risks to the ITW/AA network based on information about mission systems and information about network connectivity.

The ITW/AA Network DAA will assign an accreditation range[1] to the ITW/AA network based on operational needs and his risk assessment.

Policy Objective 2. The ITW/AA Network Manager will manage the security of the ITW/AA network in compliance with the requirements specified by an approved network security policy.

Policy Objective 3. The ITW/AA Network DAA will allow a system to participate in the ITW/AA network only if the DAA determines that the level of risk for the ITW/AA network would remain acceptable with that system's participation.

Systems can reduce risk associated with their participation by improvements in their security features.

- Compliance with the labeling and nondisclosure requirements will reduce the disclosure risk for the ITW/AA network.

- Compliance with the integrity requirements will reduce the loss-of-integrity risk to the ITW/AA network.

- Compliance with the network management requirements for missions systems will ensure that network secrecy and integrity measures are enforced and are based on accurate information.

Policy Objective 4. The ITW/AA network security policy will be effective upon approval by the ITW/AA Network DAA and will apply to all ITW/AA network accreditations.

[1] The accreditation range is a set of authorized security levels for data transmission.

SECTION 3

TECHNICAL APPROACH TO THE NETWORK SECURITY POLICY

This section has four subsections that give the technical basis for the network security policy defined in the appendix of this document.

- Subsection 3.1 gives the technical elements on which the network security policy is based. It develops a view of the ITW/AA network useful for defining the network security policy. In developing this view, we characterize the communications systems and AISs of the network, discuss what a network interface is and how it is used for policy requirements, define input and output channels and their use, and discuss labeling of information. Each of the following subsections then uses the technical elements and viewpoint given in this subsection.
- Subsection 3.2 discusses how the policy provides for network security management.
- Subsection 3.3 discusses how the policy prevents unauthorized disclosure of information.
- Subsection 3.4 discusses how the policy maintains integrity of information.
- Subsection 3.5 discusses the scopes of the major subdivisions of the policy.

3.1 ELEMENTS OF THE TECHNICAL APPROACH

One can view the ITW/AA network from several points of view. For describing and specifying a network security policy for ITW/AA, we need a view that is simple yet comprehensive. Simplicity is obviously desirable because it supports effective communication of concepts and meanings. The view must be comprehensive, covering the current ITW/AA network as well as its likely upgrades, to protect the investment that will be made in incremental improvements and risk assessment.

Many alternatives are possible. We could look at the ITW/AA network as a data communications network, as a set of cooperating sites, or as a single large system having a complex set of information exchange protocols. Since the AISs and the communications capabilities involved are heterogeneous sets coming under various authorities, the view that treats the network as a set of cooperating AISs employing communications capabilities for information exchange appears best for specifying and applying a network security policy. Thus, our fundamental view is that security policy requirements for secrecy and integrity can be stated in terms of responsibilities of individual AISs and communications systems and in terms of constraints on pairs of communicating AISs.

3.1.1 AISs and Communications Capabilities

The AISs of ITW/AA are a heterogeneous set of widely differing data processing capabilities—sensor systems that include radar subsystems, correlation center aggregates that have a multitude of computer mainframes and message processing hardware, and user systems of various types from individual workstations to multiple-user computer mainframes. To keep the network security policy manageable, we need to use a reference term that covers all these cases and can easily be interpreted for a given context. For this reference term we use "AIS".

Automated Information System (AIS): A collection of hardware, software, and firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. An AIS may be a single computer or workstation or an aggregate of computers, workstations, servers, and communications equipment identifiable as a single system, such as a local area or wide area network.

Typically, the criterion for "identifiable as a single system" will be mission and accreditation authority. In some cases, though, the network security policy might appropriately be applied to a single unit of a collection of systems having a common mission under the same authority, such as the PAVE PAWS system.

In the ITW/AA environment, the mission systems are a principal focus of the network security policy.

Mission System: An AIS that supports an ITW/AA mission, characterized as either a core system or an affiliated system of the ITW/AA network depending on whether the mission function is primary or secondary, respectively.

However, mission systems may have occasion to communicate with AISs not involved with the ITW/AA missions. We call these systems "nonmission systems".

Nonmission System: A system having an intercomputer networking relationship with an ITW/AA mission system and being neither a core nor an affiliated system.

Since the ITW/AA mission systems generally deal with sensitive information that must be protected from unauthorized disclosure, the network security policy must take account of these nonmission systems even though they do not come under the authority of the ITW/AA Network DAA.

The ITW/AA network currently uses a number of communications systems, such as SCIS and AUTODIN, and a variety of protocols, including limited use of the TCP/IP protocol suite. Sometime in the future, information exchange between AISs may be done within the framework of the Open Systems Interconnection (OSI) protocol stack [4].

The network security policy deals with AISs and communications systems. The real systems involved are complex and complicated. To manage the complexity and complications, we abstract away the unnecessary details and state the policy in terms that can be interpreted for a variety of situations. Therefore, we view all data communications relationships among the mission systems and between a mission system and a nonmission system as communications capabilities supported by communications systems.

Communications capability: A capability that enables, supports, or implements information exchange between two AISs.

The communications capability is the fundamental relationship on which we build the network security policy, as depicted in figure 1.

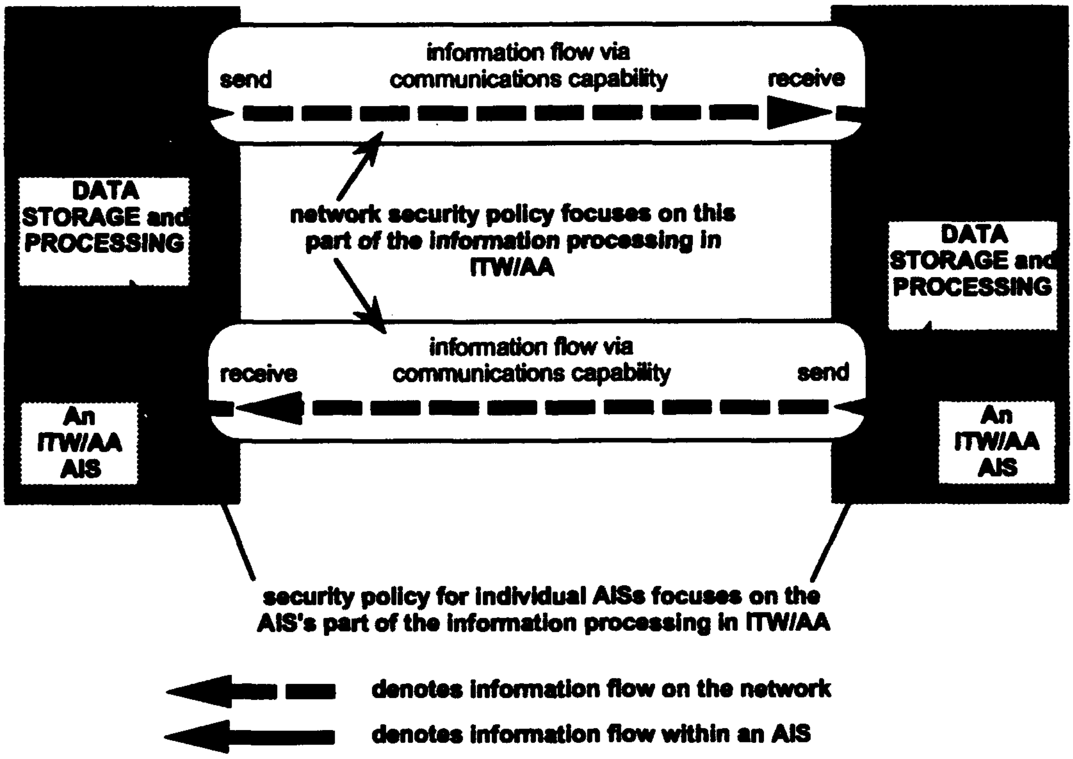

information flow via communications capability
send
receive
DATA STORAGE and PROCESSING
network security policy focuses on this part of the information processing in ITW/AA
DATA STORAGE and PROCESSING
information flow via communications capability
receive
send
An ITW/AA AIS
An ITW/AA AIS
security policy for individual AISs focuses on the AIS's part of the information processing in ITW/AA
denotes information flow on the network
denotes information flow within an AIS

Figure 1. Fundamental Technical View for Defining Policy

We use the term "liaison" in this context to refer to an instance of a communications capability between two AISs.

Liaison: A networking relationship between two AISs that exists for a time needed to transfer information.

Liaisons can be realized in a variety of ways. Two AISs can use a specialized protocol on a dedicated communications system for logical one-way, continuous reporting of sensor data. AISs can also use general intercomputer networking protocols such as File Transfer Protocol (FTP) over a packet-switched network. The capability to send a message from one AIS to another via AUTODIN is also referred to as a liaison. In the specification of the network security policy, we use only the term "liaison" to refer to intercomputer networking relationships among AISs. Thus, a requirement specified in terms of "liaisons" applies to intercomputer networking by "connections," "connectionless protocols," "dedicated circuits," "delivery services," and so forth.

3.1.2 Network Interfaces

To use a communications capability, a computer must have an appropriate interface to that capability. In the ITW/AA system there can be many different kinds of interfaces. Interfacing to AUTODIN, for example, can be manual, by floppy disk or hardcopy carried by a messenger, or automated in a variety of ways. For some systems, their interface to a particular communications system may be through an intermediary system. Others may employ in-board networking protocols to directly access a data communications system. We want the network security policy governing all these situations to be stated in simple terms that can be interpreted easily and correctly for each situation that may arise in practice. For this purpose we use the notion of a network interface.

Network Interface: The capability of an AIS to exchange information with other AISs. The capability, totally contained within the AIS and a part of it, may consist of hardware, software, or a combination of hardware and software. A network interface implements the necessary protocols, including security features, needed to enable data communications.

Notice that an AIS using an intermediary system to gain access to a communications system has a network interface, as just defined, that is totally contained within itself. Although this interface provides communications only with the intermediary system, for interpreting policy requirements with respect to the communications system we can consider it an interface to the communications capability provided by the communications system on the other side of the intermediary system. At a more detailed level of consideration, we may wish to view the network interface in terms of the communications capability between the AIS and the intermediary system.

For network security purposes, the network interface acts as a surrogate for its containing AIS. Although it may have a number of attributes relevant to intercomputer networking, its principal attribute of interest for the network security policy is its accreditation range.

An accreditation range for a network interface is a set of security levels for transmission of data between an AIS and a network. This accreditation range is always a subset of the accreditation range of the network. The range is normally also a subset of the accreditation range of the AIS. Denoting an accreditation range of Unclassified and Secret as [U, S], consider the following example. The network's accreditation range is [U, S], the AIS's range is [U, S], and one of its network interfaces has a range [S]. In this example, the network interface is single-level, authorized to transmit and receive Secret information. Typically, the network interfaces of system high systems will have accreditation ranges that are simply [S].

However, in special situations a network interface's range might be multilevel while its owning AIS's range is single-level. In such a case, the highest level in the network interface's accreditation range must be less than or equal to the single level in the accreditation range of the AIS. As before, suppose the network's accreditation range is [U, S]. However, let the AIS's range be [S] instead of multilevel and let the network interface's range be [U, S]. Authorization for this setup might be based on a restricted trust capability in the AIS. Restricted trust is authorized dependence on the correctness and strength of a particular capability, mechanism, or portion of a computer system, as opposed to reliance on the trusted computing base of the computer system. A certified computer program that changes the marking on information from Secret to Unclassified would serve in the example we just outlined.

The fundamental technical view shown in earlier figure 1 is further elaborated with the addition of network interfaces as shown in figure 2.

3.1.3 Input and Output Channels

One further stage of elaboration is useful for the network security policy. We model the interfaces of an AIS to the networking capabilities as input channels and output channels. Input and output channels are specific communications relationships of an AIS with other AISs. They are created and managed by an AIS's network interfaces.

Input Channel: A resource of an AIS's network interface through which the AIS can receive data from the network.

Output Channel: A resource of an AIS's network interface through which the AIS can transmit data to the network.

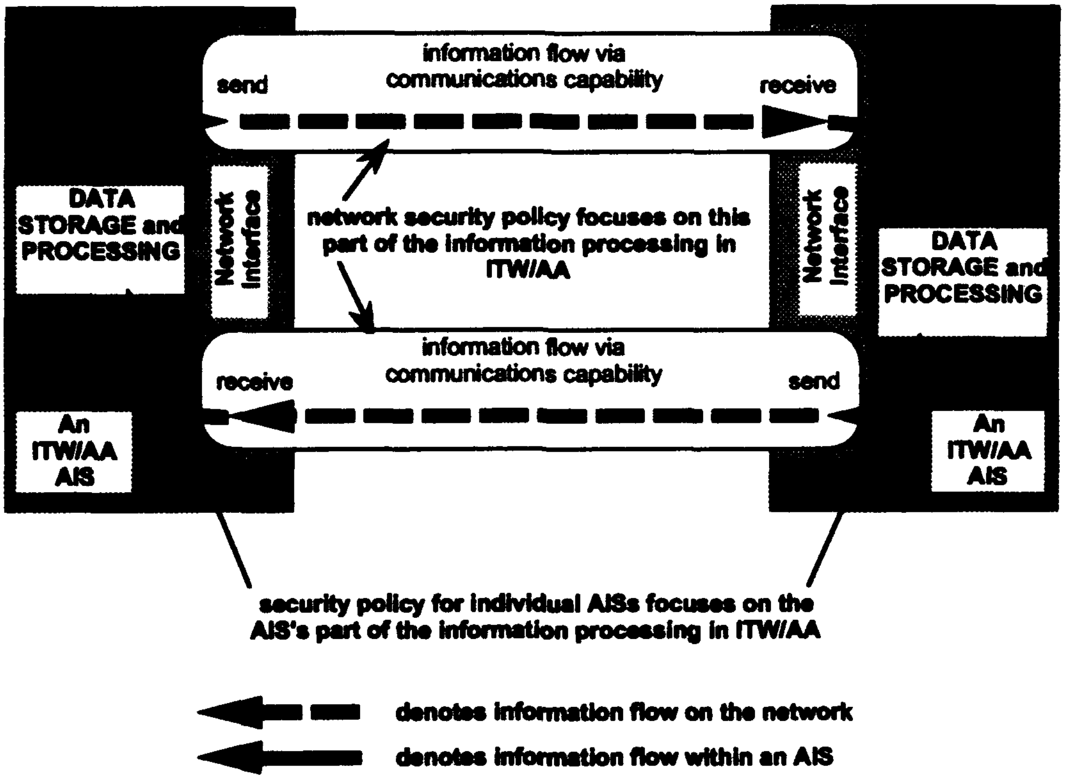

information flow via communications capability
send
receive
DATA STORAGE and PROCESSING
Network Interface
network security policy focuses on this part of the information processing in ITW/AA
Network Interface
DATA STORAGE and PROCESSING
information flow via communications capability
receive
send
An ITW/AA AIS
An ITW/AA AIS
security policy for individual AISs focuses on the AIS's part of the information processing in ITW/AA
denotes information flow on the network
denotes information flow within an AIS

Figure 2. Elaborated Technical View for Defining Policy

Input and output channels, resources of a network interface, are contained within their network interface. Network interfaces, the capability of an AIS to communicate, are contained within their AIS. A TCP connection at an AIS would be modeled by a network interface (TCP/IP and supporting protocol interpreters) of the AIS providing and managing two channels for the connection, one input channel, for receiving data on the TCP connection, and one output channel, for transmitting data on the connection. Similarly, an AIS's ability to receive sensor-data inputs on a continuous basis over a dedicated line providing one-way communications would be modeled as an input channel managed by a network interface. In this situation the network interface might manage hundreds of dedicated-service input channels.

AISs and network interfaces, as we have seen, have accreditation ranges. Input and output channels are dynamic in that they are created and deleted by their managing network interfaces, so they do not have accreditation ranges, which are static assignments of security levels. Instead, input and output channels are dynamically assigned operating security levels by their network interfaces. An operating security level is a security level in the accreditation range of the network interface at which the channel will operate. A channel can be assigned to operate at a single level or at multiple levels so that channels can be viewed as single-level or multilevel.

The elaborated technical view shown in earlier figure 2 is further elaborated with the addition of input and output channels as shown in figure 3.

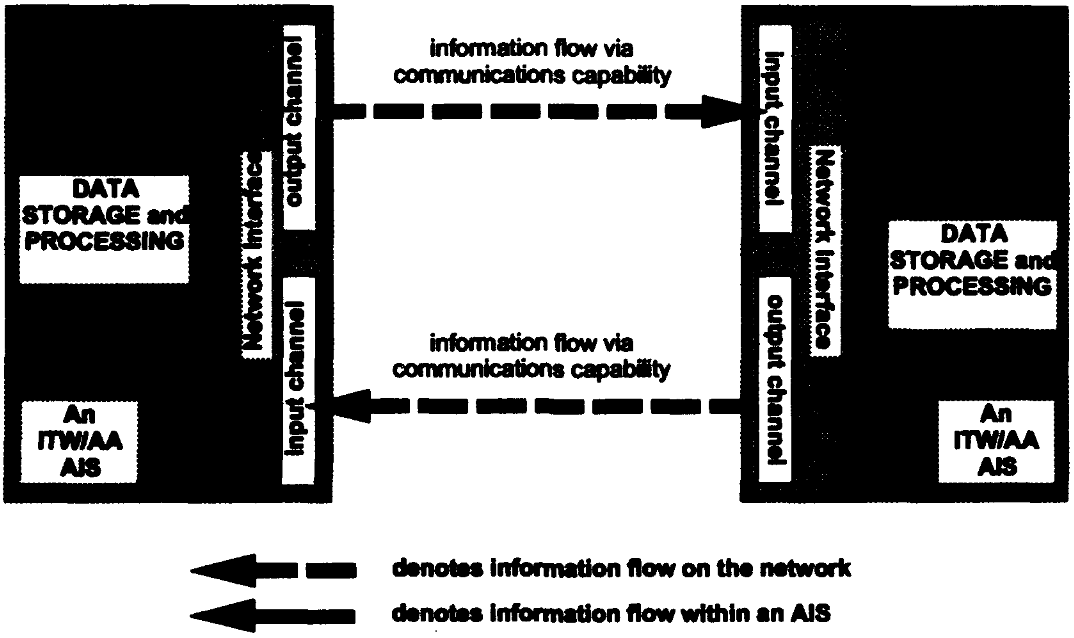

DATA STORAGE and PROCESSING
An ITW/AA AIS
Network Interface
output channel
input channel
information flow via communications capability
information flow via communications capability
input channel
output channel
Network Interface
DATA STORAGE and PROCESSING
An ITW/AA AIS
denotes information flow on the network
denotes information flow within an AIS

Figure 3. View for Network Security Policy at Input/Output Channel Level

Much of the network security policy defined in the appendix is in terms of input and output channels. Information transmission in ITW/AA is viewed as a send of a unit of information by an output channel to a communications capability, a transport of the unit of information by the communications capability to an input channel, and a receive of the unit of information by the input channel.

The policy requirements are based on the following characterization of compatibility of an input-output channel pair.

Characterization of compatibility of channels: An input and an output channel are compatible when

- The channels operate at the same security level or set of security levels. Clearly this implies that their network interfaces must have the security level or set of security levels in common.
- The communications system that supports the communications capability between the channels has been approved for carrying data that is classified at the security level(s) at which the channels are operating.
- The intercomputer networking protocols used for the input-output channel pair, or the data communications system they are using, or both together support data communications integrity, protocol integrity, and authentication (generally, the integrity requirements of the network security policy).
- The AISs of the input-output channel pair satisfy the labeling requirements of the network security policy in a compatible manner.

Judicious use of restricted trust in conjunction with assignment of accreditation ranges to network interfaces and input/output channels will accommodate a variety of operational needs. Consider one example: A system-high Secret system is required to send Secret data to a system-high Top Secret system. The output and input channels would operate at the Secret level and the Top Secret system would be required by the security policy governing its operation to change the classification of received data to Top Secret immediately upon receipt, since its accredited mode of operation is "system high". The Top Secret system would also have to have some form of restricted trust in place to allow it to internetwork with a Secret system at all — for example, use of a receive-only dedicated line or use of certified logically-one-way protocols. But the required flow of information can be accommodated within the bounds of the proposed network security policy.

3.1.4 Security Labels

Some requirements of the network security policy deal with labeling the information that is exchanged among the ITW/AA systems. The notion of a security label is central to these requirements.

Security Label: An information container for security attributes of an associated, controlled entity, especially for designating security levels.

In normal usage, a security label is data contained in or attached to a unit of information; this data indicates the security level of the information and may also give other handling and dissemination designators. The network security policy for ITW/AA focuses on the security level portion of a security label.

> **Security Level**: A hierarchical classification and a set of nonhierarchical categories.

The security labels referenced by the network security policy are considered trusted labels and are called explicit labels.

> **Trusted Label**: A label, associated with a unit of information, that has been certified by an approval authority. The certification allows its security attributes to be used in access control, handling, and dissemination of the information associated with the label.

> **Explicit Label**: A security label provided with a unit of information transmitted via a communications capability and having the characteristic that there is a correspondence from each required item of the ITW/AA standard network security label to an attribute in the label.

In addition to use of explicit labels for transmission of information, the network security policy allows transmission of unlabeled information via a communications capability. In this case, an explicit label must be generated by the receiver of the information and the sender must meet certain requirements to make this possible. Subsection 3.1.4.2 discusses methods for assigning an explicit label to received information.

3.1.4.1 Components of Security Labels

Defining an ITW/AA standard label is outside the scope of this policy document. Specification of a standard [5], which is expected to define an ITW/AA standard label that will be required for ITW/AA mission traffic, is being coordinated separately from the network security policy. Nevertheless, we need to characterize a standard label because many of the requirements of the proposed policy deal with security labels. Thus, to provide an interim basis for risk analysis and to have a consistent idea of the meaning of "label" for policy interpretation, we identify minimally expected ITW/AA label components in table 1. The security label components comprise a security level for information and additional markings for information handling and releasability.

Table 1. ITW/AA Label Components

Label Component	Content[2]
Label type	ITW/AA
Classification	Top Secret, Secret, Confidential, or Unclassified
Special Handling Designators[3]	NOCONTRACT, NOFORN, RD, and/or WNINTEL
Non-DOD Releasability Indicators	Up to three, as yet unspecified, such indicators are likely
Foreign Releasability Indicators	Releasable to Canada, United Kingdom, and/or several other possible countries
Categories[4]	Up to four categories appear likely
Real/Test/Exercise Indicator	Real, Test, or Exercise

The reader should interpret labeling requirements in the proposed policy given in appendix A in light of this description of security labels for ITW/AA until an ITW/AA standard label is specified.

[2] Some combinations of handling designators, releasability indicators, and categories may not be valid.

[3] There are other possible Special Handling Designators (SHDs) which could be nominated for inclusion (e.g., LIMDIS, CNWDI). The SHDs identified in the table are the only ones now used by an Integrated TW/AA system (SPADOC 4C).

[4] For example, SCI, SIOP, ESI.

3.1.4.2 Labeling Information

The network security policy focuses on the input/output channel level, as depicted in preceding figure 3, for specifying labeling requirements. The general idea is that an AIS should be able unambiguously to determine the appropriate security level of information received through the network. For this purpose, the policy allows three basic methods

- Explicit Labels
- Implicit Labeling by Information Characteristics
- Labeling by Level of Input Channel

These three methods are illustrated in the following three pictures.

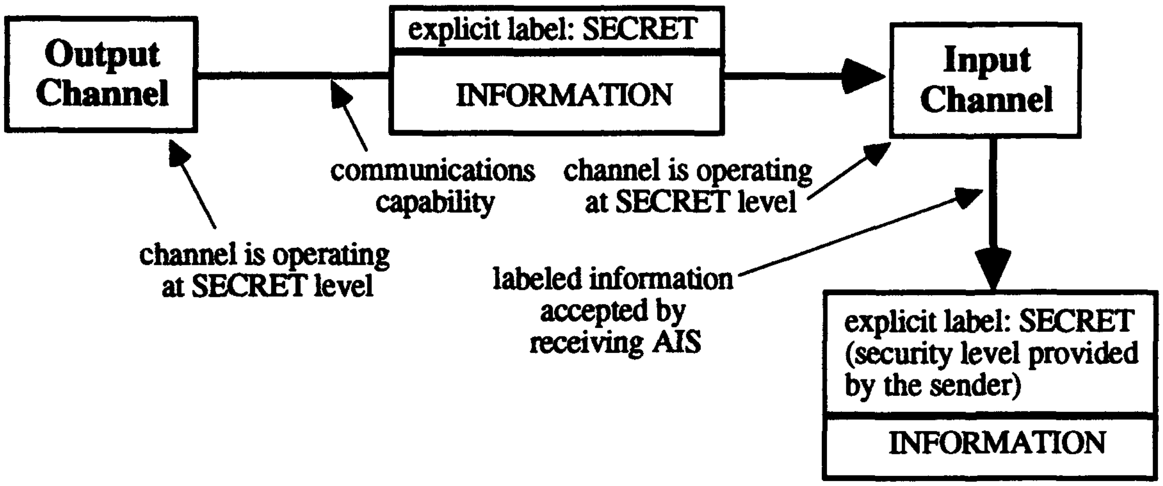

Output Channel
explicit label: SECRET
INFORMATION
Input Channel
communications capability
channel is operating at SECRET level
channel is operating at SECRET level
labeled information accepted by receiving AIS
explicit label: SECRET (security level provided by the sender)
INFORMATION

Figure 4. Labeling Information with Explicit Label Provided by Sender

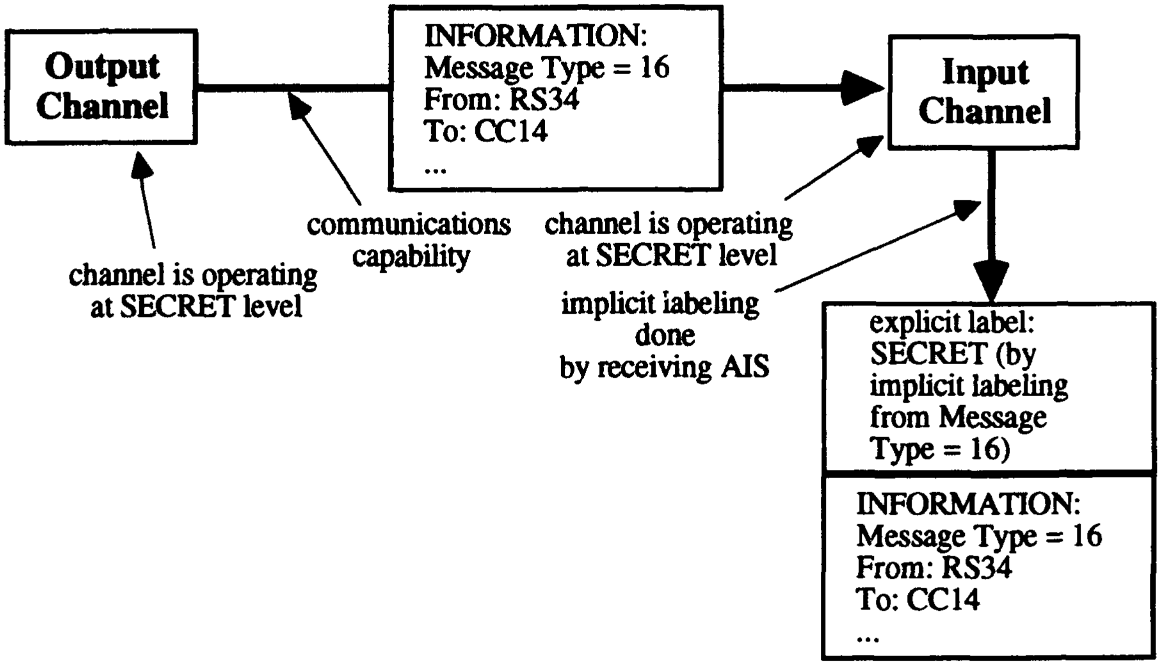

Output Channel
INFORMATION:
Message Type = 16
From: RS34
To: CC14
...
Input Channel
communications capability
channel is operating at SECRET level
channel is operating at SECRET level
implicit labeling done by receiving AIS
explicit label: SECRET (by implicit labeling from Message Type = 16)
INFORMATION:
Message Type = 16
From: RS34
To: CC14
...

Figure 5. Labeling Information by Implicit Labeling

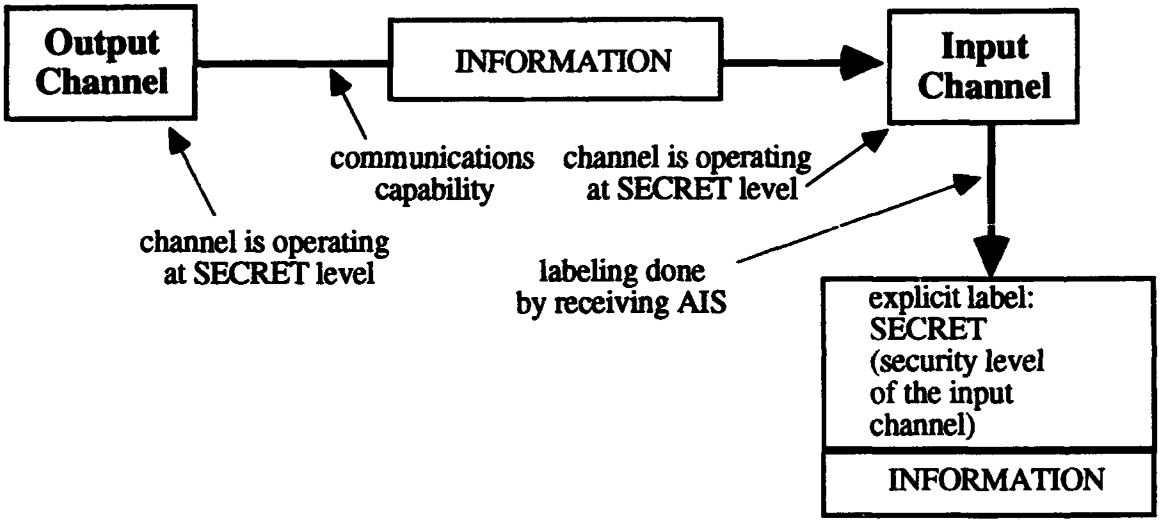

Output Channel
INFORMATION
Input Channel
communications capability
channel is operating at SECRET level
channel is operating at SECRET level
labeling done by receiving AIS
explicit label: SECRET (security level of the input channel)
INFORMATION

Figure 6. Labeling Information by Operating Level of Input Channel

Implicit labeling will be useful only in cases where all units of information received on a given input channel reliably have the needed characteristics to enable unambiguous determination of a security level.

Implicit Labeling: Generating an explicit security label for information received on an input channel based on characteristics of the data, its containing object, or its encoding. For example, satellite number or message type might reliably indicate the security level of the contained information. Encryption, an example of encoding, might reliably indicate a security level by the key used for encrypting.

Note that the process of implicit labeling can, in theory, be applied to information even if it has an explicit label; the normal use of implicit labeling in ITW/AA, however, would be for unlabeled information.

The policy for labeling given in the appendix constrains the sender of information to conform to the implied requirements of these methods. For example, for the receiver to correctly assign the operating level of its input channel to unlabeled data, the sender must be using an output channel operating at the same security level as the receiver's input channel and the sender must ensure that it transmits only information covered by that security level through its output channel. Similarly, the policy requires the receiver to check the security levels it assigns to received information to ensure that the implied constraints of the methods described above are met.

3.2 MANAGING NETWORK SECURITY

Compliance with the management-oriented requirements of the network security policy reduces the risk of unauthorized disclosure and loss of integrity in operating the ITW/AA network. Network security management requirements derive from the view that proper control of information processing in the ITW/AA system will be supported if the following conditions hold.

- Each principal agent of authority carries out a minimal set of analyses and certifications for their assigned systems.
- Proper system accreditations are maintained.
- Control of attachments to the ITW/AA network is exercised to ensure that a minimal set of safeguards for information processing is in place.
- Adequate audit information is gathered and reviewed on a continuing basis.
- System administrators are empowered to make dynamic configuration changes to achieve better operational tradeoffs during crisis or other emergencies.

This view translates into requirements in five categories

- Roles and Responsibilities
- System Accreditation
- Approval of Attachments to the ITW/AA Network
- Network Audit
- Contingency Operation

Much of the network security management depends on the availability of information about the systems involved in ITW/AA intercomputer networking. This information is critical to the need for the ITW/AA Network DAA to determine whether the risks of an AIS's participation in the ITW/AA intercomputer networking are acceptable. For this reason, the proposed policy in appendix A specifies the content of a standard accreditation information document and requires that every participating system provide such a document or an approved substitute to the ITW/AA Network DAA. The policy defines the minimum information elements for a standard accreditation information document as shown in table 2.

Table 2. Minimum Accreditation Information Elements

Minimum Accreditation Information Elements
Definition of the accredited security operating mode of the AIS, including the minimum clearance level required for all classes of users.
The accreditation range of the AIS.
The accreditation range(s) of the AIS's network interface(s) to the ITW/AA network.
Description of any implicit labeling capability used by the AIS for information it receives.
Definition of explicit labels the AIS provides with information it transmits.
Description of the AIS's security features.
An assessment of the degree of assurance associated with the AIS security features.
The criticality of the system.
Identification of all physical attachments of the AIS to the ITW/AA system.
The ITW/AA missions the AIS supports.
Identification of expected application layer liaisons with both mission and nonmission systems.

3.3 PREVENTING UNAUTHORIZED DISCLOSURE

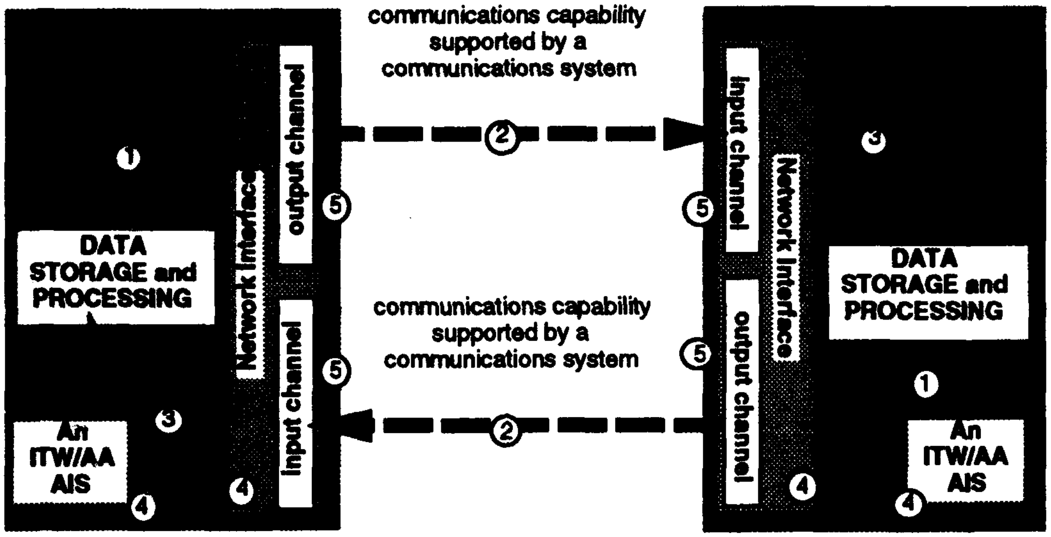
Compliance with the nondisclosure requirements of the network security policy can reduce the risk of unauthorized disclosure of information in the ITW/AA network. Nondisclosure requirements derive from the view that proper control of sensitive information in ITW/AA will be maintained if the following conditions hold.

- Each AIS protects the sensitive data it stores and processes, assigning it proper security levels and controlling access to it.
- Only information at authorized security levels is transmitted on the network.
- Proper security level identification is preserved during network transmission.
- Transmitted information is properly labeled at its destination.

This view translates into requirements in six categories

- Labels in Message Standards
- Network Interfaces
- Input Channels
- Output Channels
- Input-Output Channel Pairs
- Communications Systems

Figure 7 depicts how the policy prevents unauthorized disclosure in terms of these elements.


communications capability supported by a communications system
1
DATA STORAGE and PROCESSING
Network Interface
output channel
5
input channel
5
3
An ITW/AA AIS
4
4
2
communications capability supported by a communications system
2
input channel
5
Network Interface
3
DATA STORAGE and PROCESSING
output channel
5
1
An ITW/AA AIS
4
4

① Information labeling: the AIS (1) labels transmitted information with an explicit label, (2) transmits unlabeled information for which the receiver can do implicit labeling, or (3) transmits unlabeled information on an appropriate single-level output channel to a corresponding single-level input channel.

② The communications systems must protect the data during transmission.

③ Information labeling: the AIS labels received information with a trusted label derived from (1) an explicit label provided with the information , (2) implicit labeling, or (3) the level of the input channel.

④ Accreditation ranges: each AIS and each network interface has a set of authorized security levels.

⑤ Operating levels: each input or output channel operates at one or more authorized security levels.

◀━ ━ denotes information flow on the network

◀━━ denotes information flow within an AIS

ⓝ relates descriptive text to the object

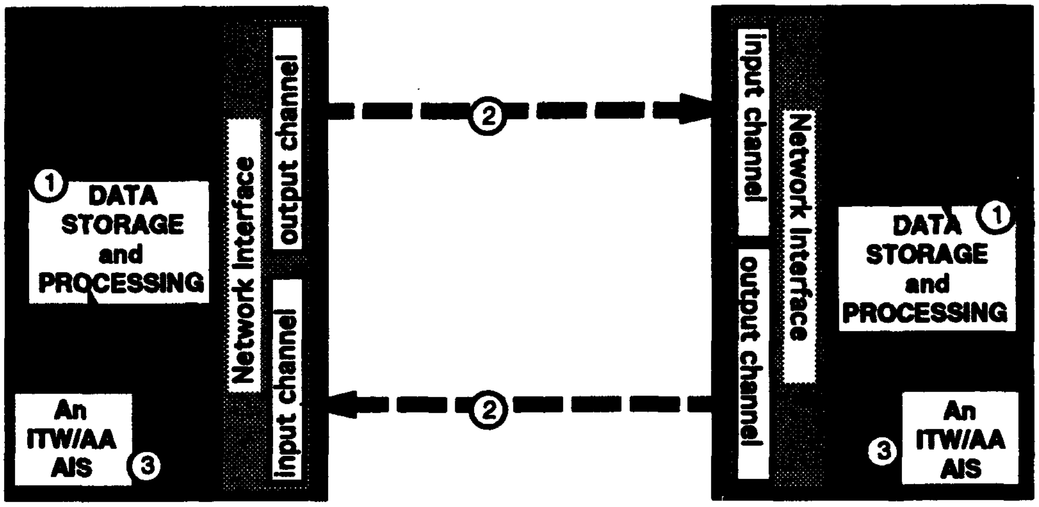
Figure 7. A Secrecy View of ITW/AA Intercomputer Networking

3.4 MAINTAINING INTEGRITY

Compliance with the integrity requirements of the network security policy can reduce the risk of loss of integrity in the ITW/AA network. Integrity requirements derive from the view that integrity of information in ITW/AA will be maintained if data integrity, protocol integrity, and authentication of senders/receivers are observed.

- Each AIS maintains the integrity of the data it stores and processes.
- Data integrity is preserved during network transmission.
- Transmitted data arrives at its proper destination.

This view is depicted in figure 8.



◄▬ ▬ denotes information flow on the network

◄▬▬ denotes information flow within an AIS

ⓝ relates descriptive text to the object concerned

① Data integrity: during storage and processing, each AIS must ensure the integrity of its data.

② Protocol integrity: data transmission protocols must ensure the integrity of transmitted data.

③ Authentication: each AIS must know its peer in network communications.

Figure 8. An Integrity View of ITW/AA Intercomputer Networking

3.5 SCOPE OF THE POLICY

The network security policy specified in the appendix has three major parts

- Managing Network Security
- Preventing Unauthorized Disclosure
- Maintaining Integrity

The requirements for managing network security generally self-define their scope of applicability and authority. For some specific requirements, the scope extends to all AISs that attach to the ITW/AA network, including nonmission systems. Generally this broad extent of applicability is restricted to the requirements governing the conditions for attaching to the ITW/AA network. Many of the network security management requirements are limited to mission systems, and some are limited to core systems only. The network audit requirements apply to all mission systems, as depicted in figure 9.

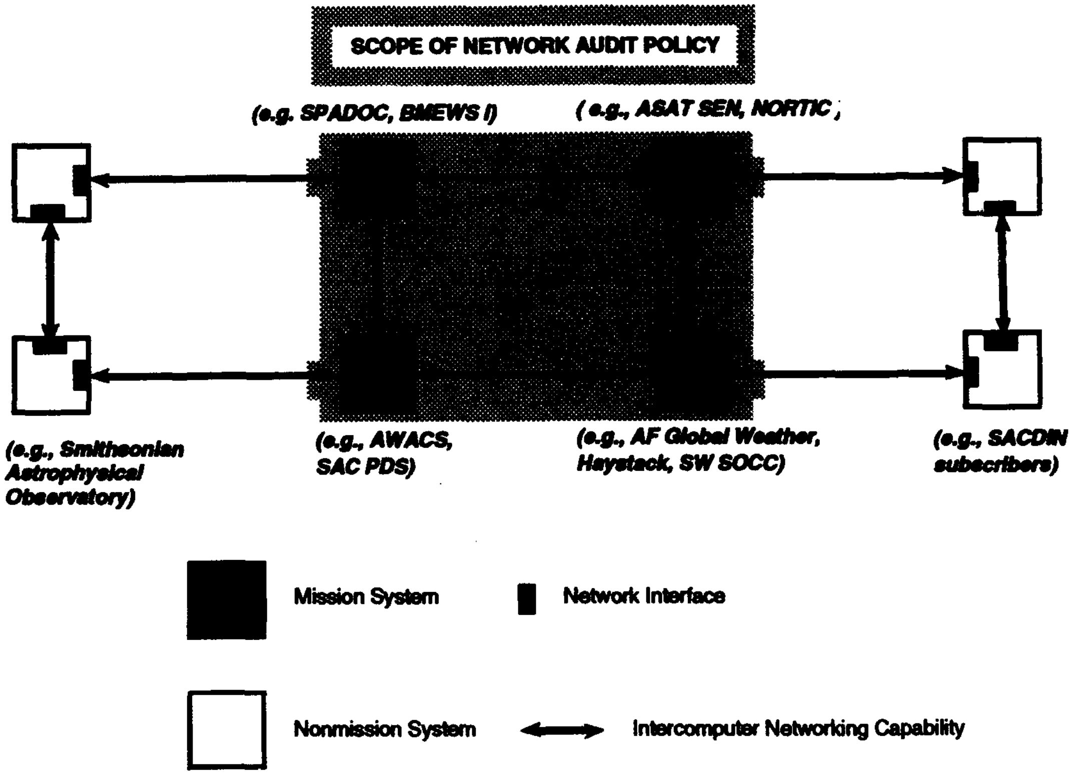

SCOPE OF NETWORK AUDIT POLICY
(e.g. SPADOC, BMEWS I)
(e.g., ASAT SEN, NORTIC ;
(e.g., Smitheonian Astrophysical Observatory)
(e.g., AWACS, SAC PDS)
(e.g., AF Global Weather, Haystack, SW SOCC)
(e.g., SACDIN subecribers)
Mission System
Network Interface
Nonmission System
Intercomputer Networking Capability

Figure 9. Scope of Network Audit Policy

The technical nondisclosure and integrity requirements have a single scope of applicability, extending up to the network interfaces of nonmission systems, as depicted in figure 10. Note that this view does not show scope of authority, which is limited as specified in the network security management requirements. The policy views a nonmission system's ITW/AA-related communications capability as terminating at a network interface having an accreditation range. This does not mean that the ITW/AA Network Manager has authority over the configuration of a nonmission system; instead, the ITW/AA Network DAA will determine whether a nonmission system's noncompliance with the technical policy warrants disabling its communications capabilities with mission systems.

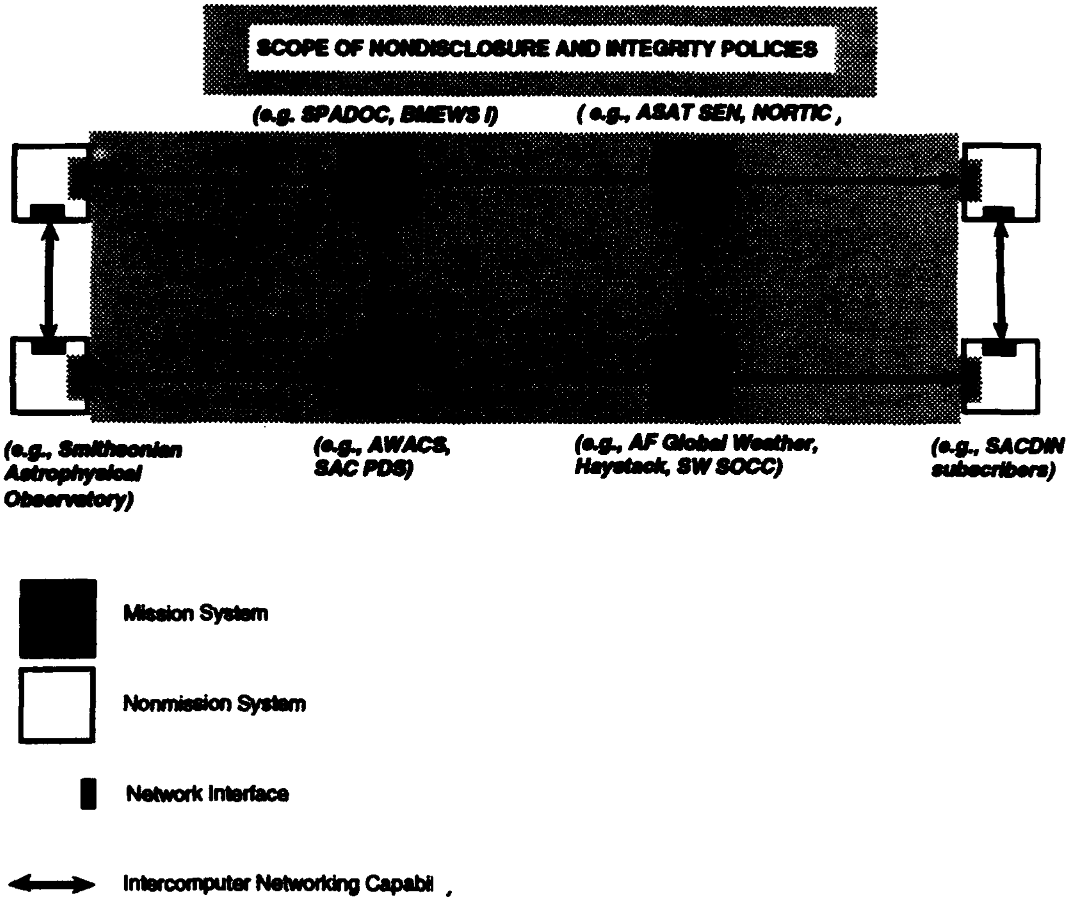

SCOPE OF NONDISCLOSURE AND INTEGRITY POLICIES
(e.g. SPADOC, BMEWS I)
(e.g., ASAT SEN, NORTIC ,
(e.g., Smithsonian Astrophysical Observatory)
(e.g., AWACS, SAC PDS)
(e.g., AF Global Weather, Haystack, SW SOCC)
(e.g., SACDIN subscribers)
Mission System
Nonmission System
Network Interface
Intercomputer Networking Capabil ,

Figure 10. Scope of Nondisclosure and Integrity Policies

SECTION 4

SUMMARY AND CONCLUSIONS

The technical approach to the proposed security policy of the appendix takes an intercomputer networking perspective. With this viewpoint we have characterized the kinds of networking service in ITW/AA both currently in use and expected as part of the evolution of the network. We have described the elements forming the basis on which the policy requirements ensure proper security management for the network, prevention of unauthorized disclosure of information, and maintenance of integrity of data. The technical elements of the approach are

- Automated Information Systems
- Communications Systems
- Network Interfaces
- Input and Output Channels
- Security Labels

We can summarize the proposed network security technical policy as follows.

- Information will be protected from unauthorized disclosure by appropriate labeling and by protection of the transmission media.

- Information will be protected from loss of integrity by protection against errors and unauthorized modification in the transmission media and by appropriate protocol integrity and authentication measures.

We have specified, in appendix A, a network security policy for ITW/AA having three major components.

- Network security management requirements: These requirements establish centralized coordination of distributed responsibility for facilitating correct and reliable protection against unauthorized disclosure and loss of integrity of information. The requirements cover roles and responsibilities, individual system accreditations, conditions for participation in the network, network audit, and contingency operation.

- Nondisclosure requirements: These requirements reduce the risk of unauthorized disclosure of ITW/AA information by labeling and label-checking for all information transmitted on the network.

- Integrity requirements: These requirements ensure that nondisclosure mechanisms function properly and that information is not altered in transiting the network.

The policy has several key features that particularly suit it to the needs of the ITW/AA network. The proposed policy

- Identifies clearly the circumstances in which security labels are required.
- Provides a security framework for implicit labeling, thereby avoiding costly development or conversion programs for systems without explicit labeling capability.
- Applies to a distributed environment; under it, network security management has distributed responsibility with centralized coordination.
- Deals effectively with liaisons of ITW/AA systems that go beyond the ITW/AA authority and security perimeter.
- Applies to various levels of abstraction; risk analysis and accreditation, for example, can ignore the composition of a communications system or can include consideration of subsystems within the communications system.
- Supports growth in the size and technology of the ITW/AA system-of-systems because it is designed with extensibility in mind.

Managing intercomputer networking security is an iterative process having these major elements

- Risk Assessment
- Allocation of Resources to Improvements
- Implementation
- Evolution

Risk assessment identifies security weaknesses and assesses their relative severity. Security weaknesses are prioritized and resources are allocated for eliminating or minimizing their effects. Implementation selects among feasible technical alternatives and develops chosen capabilities for the network. Evolution is upgrade of the network by incorporation of those capabilities as well as change in the network to accommodate changing mission and user needs as well as developing technologies. The latter changes require repetition of the process just described.

Key to the identification of security vulnerabilities is the network security policy. It provides the criteria by which a risk assessment identifies weaknesses in the form of failures to meet the criteria. The network security policy also guides the process that selects among architectural alternatives for security improvements. In this regard, it provides a set of criteria by which alternatives can be measured for their effectiveness in improving security.

And, the network security policy gives broad guidance in selecting among viable new capabilities to meet new mission and user needs.

We have provided in this document a proposed network security policy that can guide the evolution of the ITW/AA network. The main characteristics of the policy that suit it to the job are

- It is concordant with relevant national and military policies.
- It takes into explicit account the intercomputer networking topology of the current ITW/AA network.
- It is a balanced policy — the requirements are both practicable and of sufficient strength to give acceptable risk.
- Appropriate generalizations and abstractions make the policy suitable for future stages of the network.

LIST OF REFERENCES

1. *Security Requirements for Automated Information Systems (AISs)*, DODD 5200.28, December 1985, Washington, DC: Department of Defense (supersedes Security Requirements for Automated Data Processing (ADP) Systems, DODD 5200.28, 18 December 1972, amended 6 May 1977 and 29 April 1979).

2. *Computer Security Policy* (FOUO), AFR 205-16, 28 April 1989, Washington, DC: HQ USAF/SCTT (supersedes *Automated Data Processing (ADP) Security Policy, Procedures, and Responsibilities,* 1 August 1984, which in turn superseded AFR 300-8, *Automated Data Processing System (ADPS) Security Policy, Procedures, and Responsibilities,* 17 August 1979).

3. *Computer Security Policy,* AFSPACECOM Supplement 1 to AFR 205-16, 6 February 1991, Peterson AFB, CO (supersedes *NORAD/Space Command Supplement 1 to AFR 205-16,* 18 November 1985, Peterson AFB, CO: Headquarters North American Aerospace Defense Command and Headquarters Air Force Space Command; change 1, 20 June 1988).

4. *Open Systems Interconnection (OSI) Basic Reference Model,* International Standards Organization (ISO) 7498-1984, 1984, New York NY: American National Standards Association, Inc.

5. *Message Set Standard for the Integrated Tactical Warning and Attack Assessment (TW/AA) System,* DRAFT, ITW/AA-STD-1700, April 1992, Peterson AFB, CO: Directorate of Integration Engineering.

6. *Department of Defense Trusted Computer System Evaluation Criteria,* DOD 5200.28-STD, December 1985, Washington, DC: Department of Defense.

7. Comer, Douglas, 1988, *Internetworking with TCP/IP: Principles, Protocols, and Architecture,* Englewood Cliffs, New Jersey: Prentice Hall, Chapter 7.

BIBLIOGRAPHY

Disclosure of Classified Military Information to Foreign Governments and International Organizations, DODD 5230.11, 31 December 1984, Washington, DC: Department of Defense.

Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 2: Security Architecture, International Standards Organization (ISO) 7498-2, New York NY: American National Standards Association, Inc.

Information Security Program Regulation, DOD 5200.1-R/AFR 205-1, 28 April 1987, Washington, DC: HQ AFOSP/SPIB (supersedes versions dated 7 December 1982 and 1 June 1986)

Intelligence Information Systems: Standard Security Markings: DIAM 65-19, 5 July 1984, Washington, DC: Headquarters, Defense Intelligence Agency.

National Security Information, Executive Order 12356, 2 April 1982.

Security Controls on the Dissemination of Intelligence Information. DCID 1/7, 27 February 1987, Washington, DC: Director of Central Intelligence.

Security Requirements for System High and Compartmented Mode Workstations, DDS-2600-5502-87, November 1987, Washington, DC: Defense Intelligence Agency.

Trusted Network Interpretation, NCSC-TG-005, Version 1, 31 July 1987, Fort Meade, Maryland: National Computer Security Center.

APPENDIX A

NETWORK SECURITY POLICY

A.1 INTRODUCTION

This appendix contains the proposed network security policy for the ITW/AA network. The policy specifies detailed and comprehensive requirements for attaching an AIS to the ITW/AA network, preventing unauthorized disclosure of information, and maintaining integrity of information.

Statements giving policy requirements use the term "shall". Statements using terms or phrases such as "will," "is/are allowed to," "may," and "might" deal with predictions, permissions, possibilities, or description.

To facilitate reference to specific requirements, each policy requirement has a one or two character identifier in **boldface** followed by a period and a sequence number. The categories of the identifiers are as follows.

Identifier	Category
A	Audit
CP	Channel Pair
CS	Communications System
I	Integrity
IC	Input Channel
L	Label
NI	Network Interface
NM	Network Security Management
OC	Output Channel

A.2 MANAGING NETWORK SECURITY

The following categories partition the network security management requirements for participation in the ITW/AA network.

- Roles and Responsibilities — This category covers the responsibilities of the ITW/AA Network Manager, ITW/AA Network Security Manager, and AIS Computer System Security Officers.

- System Accreditation — This category covers the informational and procedural requirements governing the attachment of AISs to the ITW/AA network.
- Attachment to ITW/AA Network — This category gives the general certification requirements for attaching an AIS to the ITW/AA network.
- Network Audit — This category specifies the network security events ‘hat each mission system should audit.
- Contingency Operation — This category describes what measures the ITW/AA Network Manager should take to ensure that the network can operate responsively under contingencies such as system failure, crisis, or conventional war.

A.2.1 Roles and Responsibilities

NM.1 The ITW/AA Network DAA has overall authority for establishing, maintaining, and implementing the ITW/AA network security policy. The ITW/AA Network Manager has the responsibility to establish a network security program for implementation of the ITW/AA network security policy. The ITW/AA Network Security Manager has the responsibility to carry out the network security program.

The ITW/AA Network Security Manager reports to the ITW/AA Network Manager. The ITW/AA Network Manager reports to the ITW/AA Network DAA.

The office of AFSPACECOM/SC comprises the ITW/AA Network DAA, the ITW/AA Network Manager, and the ITW/AA Network Security Manager. However, AFSPACECOM/SC may designate individuals in the roles of ITW/AA Network Managc· and ITW/AA Network Security Manager from other appropriate offices of the Air Force.

NM.2 The NSM shall create and maintain a network security database of network security characteristics, including accreditation range and criticality of all mission systems, and authorized network attachments of both mission and nonmission systems. The NSM shall develop a security status profile for the ITW/AA network and shall report the security status to the ITW/AA Network DAA as required by the ITW/AA Network DAA.

NM.3 The NSM shall create and maintain a network audit database consisting of reports provided by mission systems under requirement **A.3** (network-security error-conditions and anomalous events). The NSM shall review the database as needed and shall report events which threaten the security of the ITW/AA network to the ITW/AA Network DAA.

NM.4 The NSM and the mission system Computer System Security Officers (CSSOs)shall have joint responsibility to establish reporting procedures for network security events and characteristics of network attachments.

NM.5 The ITW/AA Network Manager shall ensure compatibility in input-output channel pairs intended to be used for ITW/AA-related network liaisons in accordance with the following compatibility guideline.

- The channels operate at the same security level or set of security levels.

- The communications system that supports the communications capability between the channels has been approved for carrying data that is classified at the security level(s) at which the channels are operating.

- The intercomputer networking protocols used for the input-output channel pair, or the data communications system they are using, or both together meet the integrity requirements of the network policy.

- The AISs of the input-output channel pair satisfy the labeling requirements of the network security policy in a compatible manner.

NM.6 Each mission system's DAA or user organization shall provide the ITW/AA Network DAA with the name of the individual responsible for enforcing system security, usually the Computer System Security Officer (CSSO).

NM.7 Each core system's CSSO shall maintain a database of security characteristics of affiliated and nonmission systems having intercomputer networking relationships to their AIS and shall maintain audit records of changes involving their system's external intercomputer networking relationships. The CSSO shall make this information available when requested by the NSM.

A.2.2 System Accreditation Information

The ITW/AA Network DAA needs to determine whether the risks of an AIS's participation in the ITW/AA intercomputer networking are acceptable. For this reason, this network security policy defines required items of information, referred to as ITW/AA standard accreditation information.

NM.8 An ITW/AA standard accreditation information document shall contain, as a minimum, the following items of information.

Definition of the accredited security operating mode of the AIS, including the minimum clearance level required for all classes of users.

The accreditation range of the AIS.

The accreditation range(s) of the AIS's network interface(s) to the ITW/AA network.

Description of any implicit labeling capability used by the AIS for information it receives.

Definition of explicit labels the AIS provides with information it transmits.

Description of the AIS's security features.

An assessment of the degree of assurance associated with the AIS security features.

The criticality of the system.

Identification of all physical attachments of the AIS to the ITW/AA system.

The ITW/AA missions the AIS supports.

Identification of expected application layer liaisons with both mission and nonmission systems.

NM.9 An ITW/AA standard accreditation information document or an approved substitute shall be made available to the ITW/AA Network DAA for each AIS that will participate in the ITW/AA intercomputer networking. The ITW/AA Network DAA reserves approval authority for substitutes on an individual basis, but generally will use the following guideline.

Core System: Substitutes are generally not acceptable.

Affiliated System: If an affiliated system has been accredited by its DAA and an accreditation letter provides the information needed by the ITW/AA Network DAA, the letter is an acceptable substitute.[5]

Nonmission System: An accreditation letter is an acceptable substitute. In addition, certified information about the nonmission system provided by a mission system's DAA, presumably one having a necessary intercomputer networking relationship with the nonmission system, is acceptable.

[5] Note that with the exception of the last four elements of information in the standard accreditation information document, an accreditation letter normally provides this information.

NM.10 An updated ITW/AA standard accreditation information document or its approved substitute shali be made available to the ITW/AA Network DAA by each participating AIS whenever modifications will be made to that system's standard accreditation information.

A.2.3 Approval of Attachments to and Participation in the ITW/AA Network

In this context, attachment of an AIS to the ITW/AA network means physical attachment to a communications asset owned or operated by ITW/AA, while participation of an AIS may be through communications assets not owned or operated by ITW/AA.

NM.11 Any system's attachment to the ITW/AA network shall require approval of the ITW/AA Network DAA. The DAA for the attaching AIS shall certify the attachment, providing the ITW/AA Network DAA with a description of each network interface of the attachment. The description shall include the accreditation range of the network interface, the class(es) of service provided by the network interface, and identification of each class of channels supported by the network interface. The DAA for the attaching AIS shall ensure that no information is transferred through the attachment before approval of the attachment by the ITW/AA Network DAA.

NM.12 Any system's participation in the ITW/AA intercomputer networking shall require approval of the ITW/AA Network DAA. The DAA for the participating system shall certify the participation, providing the ITW/AA Network DAA with a description of each network interface used for the participation. The description shall include the accreditation range of the network interface, the class(es) of service provided by the network interface, and identification of each class of channels supported by the network interface. The DAA for the participating system shall ensure that no ITW/AA-related intercomputer networking takes place before approval of the participation by the ITW/AA Network DAA.

NM.13 If the accreditation range of any system attaching to the ITW/AA network includes a security level that is not included in the accreditation range of the ITW/AA network, the accreditation of the computer system by which the AIS attaches shall be based on a certification of security features and assurances commensurate with an evaluation class [6] that includes mandatory protection and is appropriate for the risk environment.

A.2.4 Network Audit

The following audit requirements can be met in a variety of ways, including administrative procedural methods as well as automated computer-based capabilities. Although this audit does not have to be automated, for convenience the following requirements refer to the automated system, rather than its manager, security officer, and so forth, as if the automated system were managing the audit data.

A.1 Each mission system shall have a network audit trail.

A.2 Each mission system shall audit (record in its network audit trail) the following network security events and report them to the Network Security Manager for inclusion in the network security database.

- An addition or deletion of a physical network attachment of the system.
- A change in the security parameters or intended use of any of the system's network interfaces.

A.3 Each mission system shall audit the following network security events and report them to the Network Security Manager for inclusion in the network audit database.

- Network-securit) rror-conditions associated with violations of secrecy and integrity requirements; for example, misrouted, improperly labeled[6], or modified information received on the ITW/AA network.
- Anomalous events that the system's CSSO believes imply a threat to the ITW/AA network.

A.4 For each network security event, the mission systems shall collect the following information.

- Identifiers of the systems involved in the event.
- When relevant and feasible, identification of the individual who initiated the network activity that led to the event.
- Date and time of the event.
- Type of the event — one of the four types identified in **A.2** and **A.3** above — and subtype of the event, if relevant — the particular secrecy or integrity requirement affected or violated.

[6] Note that detection of improper labeling is based on comparison of a label's contents with authorized accreditation ranges; there is no intention here to require detection of misclassification based on the information itself.

A.2.5 Contingency Operation

The relative priorities of secrecy, integrity, and availability requirements can change in different situations such as system failure, peace, crisis,[7] conventional war, or nuclear war. For this reason, the ITW/AA Network Manager will have the capability and authority to adapt the application of security measures as appropriate to the contingency.

NM.14 The ITW/AA Network Manager shall develop a contingency plan that includes enforcement and adaptation of the network security policy, shall coordinate with organizations identified in the plan to ensure that the plan can be executed, and shall present the plan to the ITW/AA Network DAA for approval.

NM.15 Each core system shall have the capability to disable intercomputer networking relationships with other systems. The ITW/AA Network Manager has the authority to activate this capability when the intercomputer networking relationships threaten the core system's mission, its security, or the mission capability of the network as a whole.

NM.16 Each core system shall have the capability to disable secrecy mechanisms protecting a network interface or liaison when necessary to minimize integrity or availability risks. The ITW/AA Network Manager has the authority to activate this capability.

NM.17 Each core system's CSSO shall define procedures for disabling intercomputer networking relationships with other systems and for disabling secrecy mechanisms that protect network interfaces or liaisons. The core system manager shall coordinate these procedures with the ITW/AA Network Manager.

A.3 PREVENTING UNAUTHORIZED DISCLOSURE

The following categories partition the requirements for preventing unauthorized disclosure of information in the ITW/AA network.

- Security Labels in Message Standards — This category identifies the requirements on the inclusion of security label specifications in current and future message standards for ITW/AA.

- Network Interfaces — This category specifies policy on accreditation ranges and use of network interfaces.

[7] Crisis is not a contingency referred to explicitly in AFR 205-16, but this policy provides the ITW/AA Network Manager with a basis for taking action related to, for example, a change in DEFCON short of actual hostilities.

- Input Channels — This category gives the policy on the use of input channels, relating security levels of channels to the accreditation ranges of the network and the AISs that use the network. It states the policy for labeling information that is received from the network, relating security levels of channels, information sent/received on the channels, and storage objects in the AISs.

- Output Channels — This category gives the policy on the use of output channels, relating security levels of channels to the accreditation ranges of the network and the AISs that use the network. It states the policy for labeling information that is transmitted on the network, relating security levels of channels, information sent/received on the channels, and storage objects in the AISs.

- Input-Output Channel Pairs — This category specifies additional constraints to be met in matching an input channel of one AIS with an output channel of another AIS.

- Communications Systems — This category gives the policy on protecting communications systems to ensure adequate support to the nondisclosure and integrity requirements for input and output channels.

A.3.1 Security Labels in Message Standards

L.1 Each message standard currently in use in ITW/AA shall be augmented by the following information

- Whether a security label is associated with the message.

- If a security label is associated with the message, whether and how each component of the ITW/AA standard label (separately defined) can be determined from the message's label.

- If a security label is not associated with the message, whether the message standard supports implicit labeling (that is, assigning an explicit label to the received message, by the receiver, on the basis of characteristics of the message).

L.2 Each new ITW/AA message standard shall accommodate the minimum requirements specified by the ITW/AA standard label by use of an explicit label. The message standard shall describe how each required component of the ITW/AA standard label can be determined from the message's label.

A.3.2 Network Interfaces

NI.1 Each network interface of an AIS shall have an accreditation range. The accreditation range of a network interface shall be a subset of the accreditation range of the ITW/AA network. The network interface is called "single-level" if its range consists of one security level; otherwise it is called "multilevel."

NI.2 An ITW/AA AIS's DAA shall require certification for each of the AIS' network interfaces that the normal use of the network interface will involve information that can appropriately be handled according to the security level(s) of the network interface's accreditation range.

A.3.3 Input Channels

IC.1 Each input channel of an AIS shall operate at a security level or levels contained in the accreditation range of its implementing network interface. The input channel is called "single-level" if it operates at a single security level; otherwise it is called "multilevel."

IC.2 The AIS's DAA shall require certification for each input channel that the normal use of the input channel will involve information that can appropriately be handled according to the security level(s) at which the input channel will operate.

IC.3 The AIS's DAA shall require certification that the normal use of each input channel will be one of, but not a mix of, the following three cases.

Case 1: Information received in the channel will have explicit labels. In this case the channel is called an explicit-label input channel. An explicit-label input channel may be either single-level or multilevel.

Case 2: Implicit labeling, based on characteristics of the received information, can reliably be used for information received in the channel. In this case the channel is called an implicit-labeling input channel. An implicit-labeling input channel may be either single-level or multilevel.

Case 3: The channel is a single-level channel, information received in the channel will be unlabeled, and implicit labeling cannot be used. In this case the channel is called a no-label input channel.

IC.4 If information received in an explicit-label input channel has an explicit label whose security level is not equal to the security level, for a single-level input channel, or one of the security levels, for a multilevel input channel, at which the input channel is operating, the receiving AIS shall record this network-security error-condition in its network audit trail, including an indication that the received information had an explicit label and that the channel was an explicit-label input channel. The AIS's DAA shall determine what additional action must be taken in the AIS to ensure that the error-condition does not persist[8].

IC.5 If information received in an explicit-label input channel has no explicit label, the receiving AIS shall record this network-security error-condition in its network audit trail, including an indication that the received information had no explicit label and that the channel was an explicit-label input channel. The AIS's DAA shall determine what additional action must be taken in the AIS to ensure that the error-condition does not persist.

IC.6 If implicit labeling of information received in an implicit-labeling input channel results in a security level that is not equal to the security level, for a single-level input channel, or one of the security levels, for a multilevel input channel, at which the input channel is operating, the AIS shall record this network-security error-condition in its network audit trail, including an indication that implicit labeling for the received information resulted in an invalid level and that the channel was an implicit-labeling input channel. The AIS's DAA shall determine what additional action must be taken in the AIS to ensure that the error-condition does not persist.

IC.7 If implicit labeling of information received in an implicit-labeling input channel cannot be done successfully, the AIS shall record this network-security error-condition in its network audit trail, including an indication that implicit labeling for the received information could not be done and that the channel was an implicit-labeling input channel. The AIS's DAA shall determine what additional action must be taken in the AIS to ensure that the error-condition does not persist.

IC.8 The receiving AIS shall assign to information received in an explicit-label input channel a security label having a security level equal to the level in the explicit label associated with the information.

IC.9 The receiving AIS shall assign to information received in an implicit-labeling input channel a security label having a security level equal to the level generated by the implicit labeling process it has applied to the information.

[8] Specification of procedures for "decontaminating" the system in such circumstances is outside the scope of the network security policy. Regulations deriving from 5200.28 are, of course, relevant and expected to be complied with in this area. One course of action for the AIS, which avoids denial of service, is to assign a "safe" (system-high) security level to the data and tag it for manual review. This might be the normal procedure to follow. However, the AIS might be required to delete the received data or even temporarily shut down, depending on specific circumstances, its accreditation range, its data processing capabilities, and the risk environment.

IC.10 The receiving AIS shall assign to information received in a no-label input channel a security label having a security level equal to the level at which the input channel is operating.

A.3.4 Output Channels

OC.1 Each output channel of an AIS shall operate at a security level or levels contained in the accreditation range of its implementing network interface. The output channel is called "single-level" if it operates at a single security level, otherwise it is called "multilevel."

OC.2 The AIS's DAA shall have certification for each output channel that the normal use of the output channel will involve information that can appropriately be handled according to the security level(s) at which the output channel will operate.

OC.3 The AIS's DAA shall have certification that the normal use of each output channel will be one of, but not a mix of, the following three cases.

Case 1: Information transmitted in the channel will have explicit labels. In this case the channel is called an explicit-label output channel. An explicit-label output channel may be either single-level or multilevel.

Case 2: Information transmitted in the channel will reliably have known characteristics that enable implicit labeling by the receiver. In this case the channel is called an implicit-labeling output channel. An implicit-labeling output channel may be either single-level or multilevel.

Case 3: The channel is a single-level channel, information transmitted in the channel will be unlabeled, and implicit labeling cannot be used by the receiver. In this case the channel is called a no-label output channel.

OC.4 The AIS shall ensure that only appropriate information is transmitted on an output channel. Information is appropriate to the channel when its actual security level is appropriately represented by the level in an explicit label assigned to it on the channel, by the level that results from implicit labeling, or by the level at which the channel is operating for a no-label output channel.

OC.5 An AIS shall associate an explicit label with information transmitted in an explicit-label output channel. The AIS shall ensure that the security level in the explicit label equals the security level, for a single-level output channel, or one of the security levels, for a multilevel output channel, at which the output channel is operating.

OC.6 The AIS shall transmit in an implicit-labeling output channel, only information for which implicit labeling can reliably be done by the receiver. The security levels resulting from implicit labeling shall be equal to the security level, for a single-level output channel, or one of the security levels, for a multilevel output channel, at which the output channel is operating.

OC.7 The AIS shall have ascertained before establishing a liaison with the receiving AIS via a no-label output channel that the receiver will use a single-level input channel whose security level is equal to the security level at which the no-label output channel is operating.

A.3.5 Input-Output Channel Pairs

CP.1 Both channels of an input-output channel pair shall be operating in the same mode, either single-level or multilevel, and shall be operating at the same security level(s).

A.3.6 Communications Systems

CS.1 Each communications system supporting the ITW/AA network shall be protected for transmission of data in accordance with its intended use. The intended use of a communications system is determined by the output channels and input channels for which it provides communications services. Thus, the communications system's protection shall be suitable for the highest level in the accreditation ranges of the output channels it services.

CS.2 Each communications system supporting the ITW/AA network shall be capable of supporting the integrity requirements of liaisons it will support when employed for its intended use.

A.4 MAINTAINING INTEGRITY

The following categories partition the requirements for maintaining integrity of information in the ITW/AA network.

- **Data Integrity** — This category denotes requirements for "processing integrity" — the integrity of data during storage and processing by an AIS. This includes protection from unauthorized, improper, and accidental modification of information and protection from improper mixing of types of information.

- **Protocol Integrity** — This category gives requirements for data communications and protocol integrity, such as protection against unauthorized modification, sometimes called "sealing," and protection against undetected loss/repetition, sometimes called "sequencing."

- **Authentication of Sender/Receiver** — This category identifies requirements for ensuring that data arrives at its intended destination, sometimes called "stamping," and that it came from its apparent source, sometimes called "signing."

A.4.1 Data Integrity

I.1 An AIS shall have the capability to protect its data from unauthorized modification.

I.2 An AIS shall have the capability reliably to distinguish Real, Test, and Exercise Data. The system may do this by physical separation, by a trusted label, or by some combination of these and other methods.

A.4.2 Protocol Integrity

I.3 Data communications integrity — protection against modification of data during transmission — shall be provided for ITW/AA intercomputer networking. This can be implemented by communications systems or by protocol interpreters used by the communicating AISs or by any combination.

I.4 Protocol integrity — protection against undetected insertion or deletion of data during transmission — shall be provided for ITW/AA intercomputer networking. This can be implemented by communications systems or by protocol interpreters used by the communicating AISs or by any combination.

A.4.3 Authentication

I.5 Data stamping — ensuring that data arrives at its intended destination — shall be provided for ITW/AA intercomputer networking. This can be implemented by communications systems or by protocol interpreters used by the communicating AISs, such as by peer authentication, or by any combination.

I.6 Data signing — ensuring that data came from its putative source — shall be provided for ITW/AA intercomputer networking. This can be implemented by communications systems or by protocol interpreters used by the communicating AISs, such as by peer authentication, or by any combination.

GLOSSARY

ACRONYMS

ADCCP	Advanced Data Communications Control Procedures
AFGWC	Air Force Global Weather Central
AFR	Air Force Regulation
AFSPACECOM	Air Force Space Command
AIS	Automated Information System
AUTODIN	Automated Digital Network
CCPDS-R	Command Center Processing and Display System - Replacement
CSSO	Computer System Security Officer
DAA	Designated Approving Authority
DODD	Department of Defense Directive
DOD	Department of Defense
ITW/AA	Integrated Tactical Warning and Attack Assessment
NOCONTRACT	No *Contractor*
NOFORN	Not Releasable to Foreign Nationals
NORAD	North American Aerospace Defense Command
NSM	Network Security Manager
RD	Restricted Data
SIOP	Single Integrated Operational Plan
STRATCOM	Strategic and Tactical Command
SW SOCC	Southwest Sector Operations Control Center
TCB	Trusted Computing Base
USSPACECOM	United States Space Command
WNINTEL	Warning Notice-Intelligence Sources or Methods Involved

TECHNICAL TERMS

Accreditation Mode: See **security mode of operations**.

Accreditation Range of a Network: A set of security levels for data transmission. The accreditation range includes the security levels that the accreditation authority believes the network can adequately manage.

Accreditation Range of an AIS: A set of security levels for data storage and processing. The accreditation range includes the security levels that the accreditation authority believes the AIS can adequately manage. The AIS is considered adequately to manage a security level if it can reliably distinguish and separate data of that security level from data of other security levels with an acceptable amount of risk.

Accreditation Range of a Network Interface (between an AIS and a network): A set of security levels for transmission of data between an AIS and a network. This accreditation range is a subset of the accreditation range of the network. The range is normally also a subset of the accreditation range of the AIS. In special cases, a multilevel range may only be bounded by the accreditation range of a single-level AIS — that is, the highest level in the network interface's accreditation range is less than or equal to the accreditation range (single level) of the AIS. The accreditation range includes only those security levels that the accreditation authority for the AIS has approved for transmission of data on the network.

Affiliated System: A system that has a secondary function of performing one or more of the ITW/AA missions. Earlier MITRE documents defined such a system as an "external" system.

Association (intercomputer networking): A connectionless liaison. For example, a liaison using User Datagram Protocol (UDP) or Internet Protocol (IP) of the DOD protocol suite or a liaison for delivering an AUTODIN message. See **connectionless service**.

Attachment: Physical and electrical connection of an AIS to data communications assets owned and operated by the ITW/AA Network for purposes of intercomputer networking.

Audit Trail: A chronological record of system activities sufficient to enable reconstruction, review, or examination of the environments and activities surrounding or leading to a class of operations, procedures, conditions, or events.

Automated Information System (AIS): A collection of hardware, software, and firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. An AIS may be a single computer or workstation or an aggregate of computers, workstations, servers, and communications equipment identifiable as a single system, such as a local area or wide area network.

Category: A restrictive designation that has been applied to classified or unclassified data as a means of increasing the protection of the data and further restricting access to the data.

Communications Capability: A capability that enables, supports, or implements information exchange between two AISs. In modeling an intercomputer network, a line of a graph is called a "communications capability" to suggest a communications capability between two nodes. For ITW/AA intercomputer networking, a communications capability can represent a communications system or a liaison.

Communication(s) Channel: This term was used in project documentation before October 1992 to designate either a communications capability or a communications system, as in the strawman security policy of May 1992.

Communications Network: A set of electronic communications media and components attached to those media whose responsibility is the transmission of data between computer systems.

Communications System: A set of communications media, communications devices, and AISs that provide data exchange among external computer systems. AISs in the communications system may also perform communications-related processing on the data being transmitted.

Connection (intercomputer networking): A liaison using an established data communications path, where the path lies between two protocol modules that provide reliable stream delivery service. From the point of view of application programs that use the service, the connection is a liaison established by a transport-layer protocol. The liaison can be defined by the ports (input/output channels) employed by the application programs.

Connection-oriented Communication: Transmission of information from one protocol entity to another using a connection.

Connectionless Communication: Transmission of information from one protocol entity to another using a connectionless service.

Connectionless Service[9]: The fundamental service provided in today's large packet-switched networks like MILNET consists of an unreliable, best-effort, connectionless packet delivery system. This service is provided by the network layer in both the TCP/IP suite and the ISO suite of protocols. The service is called *unreliable* because delivery is

[9] This definition is adapted from the description of connectionless delivery systems given in Comer's book [7].

not guaranteed: the packet may be lost, duplicated, or delivered out of order without detection and error reporting. The service is called *best-effort* because the network protocol modules make an earnest effort to deliver packets, never discarding packets capriciously, only when resources are exhausted or fail. The service is called *connectionless* because each packet is treated independently from all others. Packets sent from one machine to another may travel different paths and may arrive in any order. Note that reliable service is normally provided, as in MILNET, by higher layer protocols, as in the TCP/IP and ISO protocols. IP provides network layer connectionless service; TCP uses IP to provide connection-oriented, reliable service.

Core System: A system whose primary function is one or more of the ITW/AA missions.

Criticality: A rating assigned to a system to indicate its importance to the national defense mission (see AFR-205-16).

Data Integrity: Integrity of data: data that has not been altered or destroyed in a deliberate or accidental unauthorized manner is said to have integrity. In communications systems, data integrity is a measure of data communications performance indicating the sparsity, or, ideally, the absence, of undetected errors.

Dedicated Security Mode: A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. [DODD 5200.28]

Dominate: Security level S_1 is said to dominate security level S_2 if the hierarchical classification of S_1 is greater than or equal to that of S_2 and the nonhierarchical categories of S_1 include all those of S_2 as a subset. More generally, if S_1 and S_2 are levels from any partially ordered set of security attributes $(L, \leq)$, then S1 dominates S_2 if and only if $S_2 \leq S_1$. Security levels include only classifications and categories. Thus, the "dominate" relation is not defined for dissemination and handling controls.

Explicit Label: A security label provided with a unit of information transmitted via a communications capability and having the characteristic that there is a correspondence from each required item of the ITW/AA standard network security label to an attribute in the label.

Implicit Labeling: Generating an explicit security label for information received on an input channel based on characteristics of the data, its containing object, or its encoding. For example, satellite number or message type might reliably indicate the security level of the contained information. Encryption, an example of encoding, might reliably indicate a security level by the key used for encrypting. Note that the process of implicit labeling can, in theory, be applied to information even if it has an explicit label; the normal use of implicit labeling in ITW/AA, however, would be for unlabeled information.

Information Label: A piece of information that accurately represents the sensitivity of the *data* in a computer process, file, or other resource (abstractly, a subject or object). An information label consists of an information level (classification and compartments) and other required security markings (for example, codewords, dissemination and control markings, and handling caveats), to be used for data labeling purposes.

Input Channel: A resource of an AIS's network interface through which the AIS can receive data from the network.

Input-Output Channel Pair: An input channel and an output channel that are paired in a networking liaison. Information transmission in a liaison is viewed as a send of a unit of information by an output channel to a communications capability, a transport of the unit of information by the communications capability to an input channel, and a receive of the unit of information by the input channel.

ITW/AA Label: A standardized security label for ITW/AA that gives a security level and handling and release markings for a unit of data.

ITW/AA Standard Label: The standard security label officially approved for use in ITW/AA. At the time of publication of this paper, a standard label definition was specified in DRAFT NORAD/USSPACECOM Standard 1700, which was in final coordination.

ITW/AA Network: The ITW/AA network consists of interrelated core and affiliated AISs and the communications networks they use to exchange data.

Label: A symbolic representation of one or more characteristics of information. In the context of the ITW/AA network, a label is normally a security label that represents the security level of the data it is associated with.

Lattice: A partially ordered set in which every pair of elements has a greatest lower bound and a least upper bound.

Liaison: A networking relationship between two AISs that exists for a time needed to transfer information. Liaisons can be realized in a variety of ways. For example, two AISs might use a specialized protocol on a dedicated communications line for one-way, continuous reporting of sensor data. Or AISs might use general networking protocols such as File Transfer Protocol (FTP) over a packet-switched network. When the DOD or OSI protocol suites are used, a liaison is either a connection or an association. See **connection** and **association.**

Mission System: A system that is either a core system or an affiliated system of the ITW/AA network.

Multilevel Input Channel: An input channel with more than one operating security level.

Multilevel Output Channel: An output channel with more than one operating security level.

Multilevel Security Mode: A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same AIS when not all users have a clearance or formal access approval for all data handled by the AIS. [DODD 5200.28]

Network Attachment: An attachment of an AIS to the ITW/AA Network.

Network Audit Database: A collection of security audit reports from mission systems. The database is maintained by the ITW/AA Network Security Manager. The reports document network-security error-conditions detected by the mission systems and anomalous events that the mission system's CSSO believes imply a threat to the ITW/AA network.

Network Audit Trail: A subset of a system's audit trail that records network-security error-conditions. An example is the part of an audit trail that records the fact that a message with an invalid explicit label was received.

Network Security Database: A collection of security information about mission systems. The database is maintained by the ITW/AA Network Security Manager. The information for each system identifies sensitivity of the system, criticality of the system, and characteristics of its authorized network attachments.

Network Interface: The capability of an AIS to exchange information with other AISs. The capability, totally contained within the AIS and a part of it, may consist of hardware, software, or a combination of hardware and software. A network interface implements the necessary protocols, including security features, needed to enable data communications. Generally, a network interface can provide resources to support multiple input and output channels.

Network-Security Error-Condition: A state of intercomputer networking affairs in violation of the network security policy and requiring corrective action. For example, getting a message with an explicit label having a security level higher than its transmitting connection constitutes a network-security error-condition for the receiving AIS, which must take corrective action to attach an appropriate label to the associated, received data.

Network: A communications network and the AISs that use it.

Nonmission System: A system having an intercomputer networking relationship with an ITW/AA mission system and being neither a core nor an affiliated system.

Operating Range of an Input or Output Channel: A set of security levels at which a channel is authorized to operate. The operating range of a channel is a subset of the accreditation range of the network interface that defines the channel.

Output Channel: A resource of an AIS's network interface through which the AIS can transmit data to the network.

Participating System: Any system that participates in the ITW/AA intercomputer networking for information exchange.

Partitioned Security Mode: A mode of operation wherein all users have the clearance, but not necessarily formal access approval and need-to-know for all data handled by the AIS. This security mode encompasses the compartmented mode defined in DCID 1/16 [DODD 5200.28].[10]

[10] AFR 205-16 defines partitioned mode as a mode where each user holds a minimum clearance of one level lower than the highest classified information processed. Since the system's level is not fixed, the two levels could either be adjacent hierarchical sensitivity levels (e.g., Secret and Confidential) or two nonhierarchical sensitivity levels (e.g., Releasable to Canada and Not Releasable).

Requirements Identifier: A category code for requirements specified in this document. Table 3 (facing page) gives the category for each code. Each requirement has a category code followed by an index number, such as **I.2** for the second integrity requirement.

Table 3. Requirements Identifiers

Code	Meaning
A	Audit
CP	Channel Pair
CS	Communications System
I	Integrity
IC	Input Channel
L	Label
NI	Network Interface
NM	Network Security Management
OC	Output Channel

Restricted Trust: Assured reliance on the correctness and strength of a well-defined capability, mechanism, or portion of a system, as opposed to reliance on the trusted computing base of the system. An example is a certified re-marking program in a computer that is not a B1 class or higher trusted computer. [B1 class: the features and assurance for "Mandatory Protection" according to DOD 5200.28-STD.]

Security Label: An information container for security attributes of an associated, controlled entity, especially for designating security levels.

Security Level: A hierarchical classification and a set of nonhierarchical categories.

Security Mode of Operations: A high-level designation of: (1) the relation between the maximum security level of data an AIS handles and the clearance, formal authorizations, and need-to-know of direct and indirect users, and (2) by implication, the security features and assurances provided by the AIS to protect against unauthorized disclosure. Specific modes are variously defined in different regulations. DODD 5200.28 defines four modes of operations: dedicated, system high, partitioned, and multilevel.

Sensitivity (of Information): An attribute of information that indicates the degree of potential damage that could result from unauthorized disclosure of the information to an individual or organization.

Sensitivity Label: This term denotes exactly the meaning intended by its definition in the TCSEC: “A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.” [TCSEC]

Single-Level Input Channel: An input channel with a single operating security level.

Single-Level Output Channel: An output channel with a single operating security level.

Special Handling Designator: A marking applied to data to serve as a guide to the proper handling of the data. In SPADOC 4C, for example, four data markings, "NOFORN", "WNINTEL", "NOCONTRACT", and "Restricted Data", serve as the basis for MAC decisions. These same markings in other contexts serve as the basis for secondary distribution of data according to need-to-know, citizenship, or other criteria.

Stream Delivery Service: When two application programs transfer large volumes of data, we view the data as a stream of bits, partitioned into 8-bit octets or bytes. The stream delivery service on the destination machine passes to the receiving application program exactly the same sequence of octets that the sender passed to it on the source machine. The stream delivery service provided by the Transmission Control Protocol (TCP) of the TCP/IP suite of protocols on the MILNET provides stream delivery service by using the lower-level Internet Protocol (IP), which provides unreliable, best-effort, connectionless service. Similarly, in the ISO suite of protocols, TP-4 builds reliable stream service on top of the unreliable connectionless service provided by ISO’s IP.

System High Security Mode: A mode of operation of an AIS wherein all users having access to the AIS have a security clearance or authorization but not necessarily need-to-know for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval [DODD 5200.28].

System: A group of related computer and communications equipment forming a functional unit, generally under a single administrative entity. Loosely, the terms "system" and "AIS" are used interchangeably.

Trusted Computing Base (TCB): The totality of protection mechanisms within a computer system — including hardware, firmware, and software — the combination of which is responsible for enforcing a security policy.

Trusted Label: A label, associated with a unit of information, that has been certified by an approval authority. The certification allows its security attributes to be used in access control, handling, and dissemination of the information associated with the label.

Unlabeled Information: Information that does not have an explicit label. For purposes of network security policy, information having only an untrusted label is considered to be unlabeled.

Untrusted Label: A label, associated with a unit of information, that has not been certified by an approval authority. See **trusted label**.

User: Any authorized person who interacts with a computer system, providing inputs or receiving outputs without mediation by another person.

INDEX